VIA FACSIMILE (703)872-9306

9D-HR-19614-Daum et al.
PATENT

Remarks

Claims 1-31 are now pending in this application. Claims 1-15 are withdrawn from consideration. Claims 16-20 and 23-31 are rejected. Claims 21 and 22 are objected to. Claims 16, 20, 21, 25, 27, 28, 29, and 30 have been amended. No new matter has been added.

Applicants respectfully submit that a copy, with Examiner's initials and signature, of an information disclosure statement (PTO-1449), filed on July 15, 2004, has not been provided with the Office Action. Applicants respectfully request that an executed copy of the information disclosure statement be provided.

In response to the restriction requirement set forth in the Office Action, Applicants confirm the provisional election made by telephone on July 16, 2004, with traverse, of Group II, including Claims 16-31, for prosecution in this case.

Reconsideration of the restriction requirement imposed under 35 U.S.C. § 121 is respectfully requested. The restriction requirement is traversed because the inventions set out by Claims 1-15 in Group I and Claims 16-31 in Group II are clearly related. Applicants submit that a thorough search and examination of Claims 1-15 would be relevant to the examination of Claims 16-31 and would not be a serious burden on the Examiner. Additionally, restriction requirements are not mandatory under 35 U.S.C. §121.

For at least the reasons set forth above, Applicants request that the restriction requirement be withdrawn.

The rejection of Claims 16-19 and 23-31 under 35 U.S.C. § 103(a) as being unpatentable over Sharrow (U.S. Patent No. 6,061,668) in view of Menezes et al., *Handbook of Applied Cryptography*, is respectfully traversed.

Sharrow describes an example of a data format used by a central management computer (10) to transmit instructions, acknowledgments, and messages to appliances and machines on a network (column 3, lines 10-15). A first component of the data format is a preamble A that identifies it as a transmission from the central management computer, which has a higher priority than transmissions from appliances (column 3, lines 15-18). Next is a routing identifier B which addresses an individual appliance or machine by its unique identification code (column 3, lines 18-20). This is followed by a data field C and message field D. The last field E contains a checksum to protect data integrity (column 3, lines 20-22). A data format is used by the appliances and machines to transmit requests for service to the central management computer, to respond to instructions from the central management computer, and to report any malfunction detected by the appliance or machine controller's diagnostics (column 3, lines 32-36). The data format used by the appliances and machines include a first field a that contains the appliance's unique identification code (column 3, lines 37-38). Next is a data field b, and the last field c contains a checksum (column 3, lines 39-40).

Menezes et al. describe a method including detecting message replay (page 399, section 10.12). The method includes associating sequence numbers with both an originator and recipient of a message (page 399, section 10.12). A sequence number (counter value) serves as a unique number identifying the message (page 399, section 10.12). Distinct sequences are customarily necessary for messages from A to B and from B to A (page 399, section 10.12). The message is accepted only if the sequence number therein has not been used previously, and satisfies an agreed policy (page 399, section 10.12). The simplest policy is that the sequence number starts at zero, is incremented sequentially, and each successive message has a number one greater than the previous one received (page 399, section 10.12).

Claim 16 recites in an appliance communication network, a method for authenticating appliance messages, the method including "maintaining at an appliance communication center a shared message counter, the shared message counter shared between the communication center

and a remotely located appliance; generating a first authentication word by applying an appliance message and the shared message counter, as stored in the communication center, to an authentication algorithm; and transmitting the appliance message and the first authentication word as an authenticated message to the appliance."

Neither Sharrow nor Menezes et al., considered alone or in combination, describe or suggest a method for authenticating appliance messages as recited in Claim 16. Specifically, neither Sharrow nor Menezes et al., considered alone or in combination, describe or suggest generating a first authentication word by applying an appliance message and the shared message counter, as stored in the communication center, to an authentication algorithm, and transmitting the appliance message and the first authentication word as an authenticated message to the appliance. Rather, Sharrow describes transmitting a data format, including a preamble A, a routing identifier B, a data field C, a message field D, and a checksum field E, used by a central management computer. The preamble A identifies a transmission as a transmission from the central management computer. The routing identifier B addresses an individual appliance or machine by its unique identification code. Sharrow also describes transmitting a data format, including a first field a, a data field b, and a checksum field c, from appliances to the central management computer. The first field a contains the appliance's unique identification code. Menezes et al. describe accepting a message only if a sequence number, such as a counter value, therein has not been used previously. The sequence number serves as a unique number identifying the message. The sequence number starts at zero, is incremented sequentially, and each successive message has a number one greater than the previous one received. Accordingly, neither Sharrow nor Menezes et al., considered alone or in combination, describe or suggest generating a first authentication word by applying an appliance message and the shared message counter to an authentication algorithm. For the reasons set forth above, Claim 16 is submitted to be patentable over Sharrow in view of Menezes et al.

Claims 17-19 and 23-24 depend from independent Claim 16. When the recitations of Claims 17-19 and 23-24 are considered in combination with the recitations of Claim 16, Applicants submit that dependent Claims 17-19 and 23-24 likewise are patentable over Sharrow in view of Menezes et al.

Claim 25 recites an appliance communication center including "network connections terminating at appliances; a processing circuit; a memory storing a plurality of shared counters, each shared counter shared between the communication center and an appliance, the memory further storing instructions for: maintaining at an appliance communication center a shared message counter, the shared message counter shared between the communication center and a remotely located appliance; generating a first authentication word by applying an appliance message and the shared message counter, as stored in the communication center, to an authentication algorithm; and transmitting the appliance message and the first authentication word as an authenticated message to the appliance."

Neither Sharrow nor Menezes et al., considered alone or in combination, describe or suggest an appliance communication center as recited in Claim 25. Specifically, neither Sharrow nor Menezes et al., considered alone or in combination, describe or suggest a memory storing instructions for generating a first authentication word by applying an appliance message and the shared message counter, as stored in the communication center, to an authentication algorithm, and transmitting the appliance message and the first authentication word as an authenticated message to the appliance. Rather, Sharrow describes transmitting a data format, including a preamble A, a routing identifier B, a data field C, a message field D, and a checksum field E, used by a central management computer. The preamble A identifies a transmission as a transmission from the central management computer. The routing identifier B addresses an individual appliance or machine by its unique identification code. Sharrow also describes transmitting a data format, including a first field a, a data field b, and a checksum field c, from appliances to the central management computer. The first field a contains the appliance's unique

identification code. Menezes et al. describe accepting a message only if a sequence number, such as a counter value, therein has not been used previously. The sequence number serves as a unique number identifying the message. The sequence number starts at zero, is incremented sequentially, and each successive message has a number one greater than the previous one received. Accordingly, neither Sharrow nor Menezes et al., considered alone or in combination, describe or suggest a memory storing instructions for generating a first authentication word by applying an appliance message and the shared message counter to an authentication algorithm. For the reasons set forth above, Claim 25 is submitted to be patentable over Sharrow in view of Menezes et al.

Claims 26 and 27 depend from independent Claim 25. When the recitations of Claims 26 and 27 are considered in combination with the recitations of Claim 27, Applicants submit that dependent Claims 26 and 27 likewise are patentable over Sharrow in view of Menezes et al.

Claim 28 recites in an appliance, an appliance message authentication device including "a processor; and a memory coupled to the processor, the memory storing instructions for execution by the processor for: receiving an authenticated message, including a first authentication word and an appliance message, at the appliance; generating a second authentication word by applying a shared message counter, as stored in the appliance, and the appliance message to an authentication algorithm; and comparing the first authentication word and the second authentication word to determine authenticity of the authenticated message."

Neither Sharrow nor Menezes et al., considered alone or in combination, describe or suggest an appliance message authentication device as recited in Claim 28. Specifically, neither Sharrow nor Menezes et al., considered alone or in combination, describe or suggest the memory storing instructions for execution by the processor for generating a second authentication word by applying a shared message counter, as stored in the appliance, and the appliance message to an authentication algorithm, and comparing the first authentication word and the second

authentication word to determine authenticity of the authenticated message. Rather, Sharrow describes transmitting a data format, including a preamble A, a routing identifier B, a data field C, a message field D, and a checksum field E, used by a central management computer. The preamble A identifies a transmission as a transmission from the central management computer. The routing identifier B addresses an individual appliance or machine by its unique identification code. Sharrow also describes transmitting a data format, including a first field a, a data field b, and a checksum field c, from appliances to the central management computer. The first field a contains the appliance's unique identification code. Menezes et al. describe accepting a message only if a sequence number, such as a counter value, therein has not been used previously. The sequence number serves as a unique number identifying the message. The sequence number starts at zero, is incremented sequentially, and each successive message has a number one greater than the previous one received. Accordingly, neither Sharrow nor Menezes et al., considered alone or in combination, describe or suggest the memory storing instructions for execution by the processor for generating a second authentication word by applying a shared message counter and the appliance message to an authentication algorithm. For the reasons set forth above, Claim 28 is submitted to be patentable over Sharrow in view of Menezes et al.

Claim 29 depends from independent Claim 28. When the recitations of Claim 29 are considered in combination with the recitations of Claim 28, Applicants submit that dependent Claim 29 likewise is patentable over Sharrow in view of Menezes et al.

Claim 30 recites in an appliance communication network, a method for authenticating appliance messages, the method including "maintaining at an appliance a shared message counter, the shared message counter shared between the appliance and a remotely located appliance communication center; generating a first authentication word by applying an appliance message and the shared message counter, as stored in the appliance, to an authentication algorithm; and transmitting the appliance message and the first authentication word as an authenticated message to the appliance communication center."

Neither Sharrow nor Menezes et al., considered alone or in combination, describe or suggest a method for authenticating appliance messages as recited in Claim 30. Specifically, neither Sharrow nor Menezes et al., considered alone or in combination, describe or suggest generating a first authentication word by applying an appliance message and the shared message counter, as stored in the appliance, to an authentication algorithm, and transmitting the appliance message and the first authentication word as an authenticated message to the appliance communication center. Rather, Sharrow describes transmitting a data format, including a preamble A, a routing identifier B, a data field C, a message field D, and a checksum field E, used by a central management computer. The preamble A identifies a transmission as a transmission from the central management computer. The routing identifier B addresses an individual appliance or machine by its unique identification code. Sharrow also describes transmitting a data format, including a first field a, a data field b, and a checksum field c, from appliances to the central management computer. The first field a contains the appliance's unique identification code. Menezes et al. describe accepting a message only if a sequence number, such as a counter value, therein has not been used previously. The sequence number serves as a unique number identifying the message. The sequence number starts at zero, is incremented sequentially, and each successive message has a number one greater than the previous one received. Accordingly, neither Sharrow nor Menezes et al., considered alone or in combination, describe or suggest generating a first authentication word by applying an appliance message and the shared message counter to an authentication algorithm. For the reasons set forth above, Claim 30 is submitted to be patentable over Sharrow in view of Menezes et al.

Claim 31 depends from independent Claim 30. When the recitations of Claim 31 are considered in combination with the recitations of Claim 30, Applicants submit that dependent Claim 31 likewise is patentable over Sharrow in view of Menezes et al.

For the reasons set forth above, Applicants respectfully request that the rejection of Claims 16-19 and 23-31 under 35 U.S.C. 103(a) be withdrawn.

The rejection of Claim 20 under 35 U.S.C. § 103(a) as being unpatentable over Sharrow in view of Menezes et al., and further in view of Kaufman et al., *Network Security: Private Communication in a Public World*, is respectfully traversed.

Sharrow and Menezes et al. are described above. Kaufman et al. describe a method including reflection. An implausible attack, but one that should be prevented, is reflection (page 242). In reflection, an attacker records a message going in one direction and replays in the other (page 242). If the same sequence number could be valid in both directions, such a message could be misinterpreted (page 242). This can be avoided by using sequence numbers in different ranges for the two directions, by having a DIRECTION BIT somewhere in the message, or by having an integrity code computed by some subtly different algorithm in the two directions (page 242). If sequence numbers are reused during a conversation, the attacker can replay an old recorded message when its sequence number recurs (page 242). The best method to prevent the attacker from replaying is to change keys periodically during the conversation (page 242). Changing keys in the middle of the conversation is known as key rollover (page 242).

Claim 20 depends indirectly from Claim 16 which recites in an appliance communication network, a method for authenticating appliance messages, the method including "maintaining at an appliance communication center a shared message counter, the shared message counter shared between the communication center and a remotely located appliance; generating a first authentication word by applying an appliance message and the shared message counter, as stored in the communication center, to an authentication algorithm; and transmitting the appliance message and the first authentication word as an authenticated message to the appliance."

None of Sharrow, Menezes et al., or Kaufman et al., considered alone or in combination, describe or suggest a method for authenticating appliance messages as recited in Claim 16. Specifically, none of Sharrow, Menezes et al., or Kaufman et al., considered alone or in combination, describe or suggest generating a first authentication word by applying an appliance

message and the shared message counter, as stored in the communication center, to an authentication algorithm, and transmitting the appliance message and the first authentication word as an authenticated message to the appliance. Rather, Sharrow describes transmitting a data format, including a preamble A, a routing identifier B, a data field C, a message field D, and a checksum field E, used by a central management computer. The preamble A identifies a transmission as a transmission from the central management computer. The routing identifier B addresses an individual appliance or machine by its unique identification code. Sharrow also describes transmitting a data format, including a first field a, a data field b, and a checksum field c, from appliances to the central management computer. The first field a contains the appliance's unique identification code. Menezes et al. describe accepting a message only if a sequence number, such as a counter value, therein has not been used previously. The sequence number serves as a unique number identifying the message. The sequence number starts at zero, is incremented sequentially, and each successive message has a number one greater than the previous one received. Kaufman et al. describe avoiding an attack by using sequence numbers in different ranges for two directions, by having a DIRECTION BIT somewhere in a message, or by having an integrity code computed by some subtly different algorithm in the two directions. Kaufman et al. also describe changing keys periodically. Accordingly, none of Sharrow, Menezes et al., or Kaufman et al., considered alone or in combination, describe or suggest generating a first authentication word by applying an appliance message and the shared message counter to an authentication algorithm. For the reasons set forth above, Claim 16 is submitted to be patentable over Sharrow in view of Menezes et al., and further in view of Kaufman et al.

When the recitations of Claim 20 are considered in combination with the recitations of Claim 16, Applicants submit that dependent Claim 26 likewise is patentable over Sharrow in view of Menezes et al., and further in view of Kaufman et al.

Moreover, Applicants respectfully submit that the 35 U.S.C. § 103 rejections of Claims 1-31 are not proper rejections. As is well established, obviousness cannot be established by

combining the teachings of the cited art to produce the claimed invention, absent some teaching, suggestion, or incentive supporting the combination. None of Sharrow, Menezes et al., or Kaufman et al., considered alone or in combination, describe or suggest the claimed combination. Furthermore, in contrast to the assertion within the Office Action, Applicants respectfully submit that it would not be obvious to one skilled in the art to combine Sharrow with Menezes et al. or Kaufman et al. because there is no motivation to combine the references suggested in the art.

As the Federal Circuit has recognized, obviousness is not established merely by combining references having different individual elements of pending claims. Ex parte Levengood, 28 U.S.P.Q.2d 1300 (Bd. Pat. App. & Inter. 1993). MPEP §2143.01. Rather, there must be some suggestion, outside of Applicants' disclosure, in the prior art to combine such references, and a reasonable expectation of success must be both found in the prior art, and not based on Applicants' disclosure. In re Vaeck, 20 U.S.P.Q.2d 1436 (Fed. Cir. 1991). In the present case, neither a suggestion or motivation to combine the prior art disclosures, nor any reasonable expectation of success has been shown.

Furthermore, it is impermissible to use the claimed invention as an instruction manual or "template" to piece together the teachings of the cited art so that the claimed invention is rendered obvious. Specifically, one cannot use hindsight reconstruction to pick and choose among isolated disclosures in the art to deprecate the claimed invention. Further, it is impermissible to pick and choose from any one reference only so much of it as will support a given position, to the exclusion of other parts necessary to the full appreciation of what such reference fairly suggests to one of ordinary skill in the art. The present 35 U.S.C. § 103 rejections are based on a combination of teachings selected from multiple patents in an attempt to arrive at the claimed invention. Specifically, Sharrow teaches transmitting a data format, including a preamble A, a routing identifier B, a data field C, a message field D, and a checksum field E, used by a central management computer. The preamble A identifies a transmission as a

transmission from the central management computer. The routing identifier B addresses an individual appliance or machine by its unique identification code. Sharrow also teaches transmitting a data format, including a first field a, a data field b, and a checksum field c, from appliances to the central management computer. The first field a contains the appliance's unique identification code. Menezes et al. teach accepting a message only if a sequence number, such as a counter value, therein has not been used previously. The sequence number serves as a unique number identifying the message. The sequence number starts at zero, is incremented sequentially, and each successive message has a number one greater than the previous one received. Kaufman et al. teach avoiding an attack by using sequence numbers in different ranges for two directions, by having a DIRECTION BIT somewhere in a message, or by having an integrity code computed by some subtly different algorithm in the two directions. Kaufman et al. also teach changing keys periodically. Because there is no teaching nor suggestion in the cited art for the combination, the 35 U.S.C. § 103 rejections appear to be based on a hindsight reconstruction in which isolated disclosures have been picked and chosen in an attempt to reject the claims of the present application. Of course, such a combination is impermissible, and for this reason Applicants request that the 35 U.S.C. § 103 rejections of Claims 1-31 be withdrawn.

Applicants respectfully traverse the statement in paragraphs 8a and 8k the office action that the checksum value meets the limitation of a first authentication word (see specification, p. 23, lines 1-2). The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). Accordingly, Applicants respectfully submit that the 35 U.S.C. § 103 rejections of Claims 1-31 cannot be based on the specification of the above-referenced patent application.

For at least the reasons set forth above, Applicants respectfully request that the 35 U.S.C. § 103 rejections of claims 1-31 be withdrawn.

VIA FACSIMILE (703)872-9306

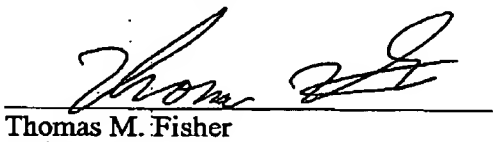
9D-HR-19614-Daum et al.
PATENT

Applicants respectfully submit that Claims 16, 25, 28, and 30 have been amended for grammatical reasons to improve readability. Applicants also respectfully submit that Claim 28 has been amended to provide antecedent basis. Applicants further respectfully submit that Claims 16, 25, 28, and 30 have not been amended to overcome the obviousness rejections.

Claims 21 and 22 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claim.

In view of the foregoing remarks, this application is believed to be in condition for allowance. Reconsideration and favorable action is respectfully solicited.

Respectfully Submitted,



Thomas M. Fisher
Registration No. 47,564
ARMSTRONG TEASDALE LLP
One Metropolitan Square, Suite 2600
St. Louis, Missouri 63102-2740
(314) 621-5070